AMENDMENTS TO THE CLAIMS

1.   (Original) A method in a data processing system for discerning corruption of an electronic ballot, comprising:

in a voter computer system:

receiving a ballot choice selected by a voter from among a set of valid ballot choices;

encoding the received ballot choice in a ballot;

encrypting the ballot;

constructing a validity proof proving that the encrypted ballot corresponds to a valid ballot choice;

sending the encrypted ballot and the validity proof to a vote collection center computer system;

in the vote collection center computer system:

receiving the encrypted ballot and validity proof;

verifying the validity proof;

only if the validity proof is successfully verified:

without decrypting the encrypted ballot, generating an encrypted vote confirmation of the encrypted ballot;

sending the encrypted vote confirmation to the voter computer system;

in the voter computer system:

receiving the encrypted vote confirmation;

decrypting the encrypted vote confirmation to obtain a vote confirmation;

displaying the obtained vote confirmation; and

if a confirmation dictionary in the user's possession does not translate the displayed vote confirmation to the ballot choice selected by the voter, determining that the ballot has been corrupted.

2.　　(Original)　The method of claim 1 wherein the encoding comprises selecting a value having a predetermined correspondence to the selected ballot choice.

3.　　(Original)　The method of claim 1 wherein the encrypting is performed using an election public key.

4.　　(Original)　The method of claim 1 wherein encrypting the ballot comprises generating an *ElGamal* pair representing the ballot.

5.　　(Original)　The method of claim 1, further comprising signing the encrypted ballot with a private key of the voter before sending the encrypted ballot to the vote collection center computer system.

6.　　(Original)　The method of claim 1 wherein the vote collection center computer system sends the encrypted vote confirmation to the voter computer system via a first communication channel, further comprising, in the vote collection center computer system, sending the confirmation dictionary to the voter via a second communications channel distinct from the first communications channel.

7.　　(Original)　The method of claim 6 wherein the confirmation dictionary is sent in response to a request from the voter.

8.　　(Original)　The method of claim 7 wherein the request includes one or more identifiers associated with the voter.

9.　　(Original)　The method of claim 6 wherein the confirmation dictionary is sent without being requested by the voter.

10.   (Original) The method of claim 6 wherein individual confirmation dictionaries are sent to each of a plurality of voters including the voter.

11.   (Original) The method of claim 1, further comprising applying a hash function to the decrypted vote confirmation before it is displayed, and wherein it is determined that the ballot has been corrupted if the confirmation dictionary in the user's possession does not translate the displayed hashed decrypted vote confirmation to the ballot choice selected by the voter.

12.   (Original) A computer-readable medium whose content cause a data processing system to discern corruption of an electronic ballot by:

 in a voter computer system:

   receiving a ballot choice selected by a voter from among a set of valid ballot choices;

   encoding the received ballot choice in a ballot;

   encrypting the ballot;

   constructing a validity proof proving that the encrypted ballot corresponds to a valid ballot choice;

   sending the encrypted ballot and the validity proof to a vote collection center computer system;

 in the vote collection center computer system:

   receiving the encrypted ballot and validity proof;

   verifying the validity proof;

   only if the validity proof is successfully verified:

     without decrypting the encrypted ballot, generating an encrypted vote confirmation of the encrypted ballot;

     sending the encrypted vote confirmation to the voter computer system;

 in the voter computer system:

   receiving the encrypted vote confirmation;

decrypting the encrypted vote confirmation;

displaying the decrypted vote confirmation; and

if a confirmation dictionary in the user's possession does not translate the displayed decrypted vote confirmation to the ballot choice selected by the voter, determining that the ballot has been corrupted.

13-28. (Cancelled)

29.   (Previously Presented) A method in a data processing system for discerning corruption of an electronic ballot, comprising, in a ballot receiving node:

receiving an encrypted ballot value from a ballot sending node, the encrypted ballot value being encrypted from a ballot value based on a voter selection using a secret not available in the ballot receiving node;

generating from the encrypted ballot value an encrypted secret value confirmation that indicates to those in possession of the secret used to encrypt the encrypted ballot value the ballot value to which the received encrypted ballot value corresponds; and

sending the encrypted secret value confirmation to the ballot sending node,

such that the encrypted secret value confirmation may be used in the ballot sending node to determine if the encrypted ballot value received at the ballot receiving node corresponds to the ballot selection made by the voter,

wherein the secret value confirmation is sent to the ballot sending node via a first communication channel, further comprising sending to the ballot sending node a confirmation dictionary via a second communication channel distinct from the first communication channel, the confirmation dictionary translating from various possible secret value confirmations to the ballot values to which they correspond.

30.   (Original) The method of claim 29 wherein the secret value confirmation is generated without decrypting the encrypted ballot value.

31.   (Cancelled)

32.   (Original) The method of claim 29 wherein the encrypted secret value confirmation is encrypted in such a manner that, in the ballot sending node, given the encrypted secret value confirmation corresponding to a selection other than the voter selection, it is intractable to generate a decrypted secret value confirmation corresponding to the voter selection.

33-50. (Cancelled)